IT – Bring Your Own Device (BYOD) Policy

Table of Contents

1. Introduction and Purpose

1.1 This policy stipulates how Bring Your Own Device (BYOD) equipment should be used at NMITE.

1.2 NMITE acknowledges and appreciates that users of our IT systems may need to use their own devices to access, store and transmit NMITE data for legitimate purposes. This policy does not therefore seek to inhibit the use of these devices, but the fact that NMITE cannot ensure that its data is always contained within a secure network with an impenetrable perimeter means that staff must take a high level of personal responsibility for the configuration and use of their own devices.

1.3 By their very nature, BYODs are considered a security risk, and should only be used in certain circumstances.

1.4 If you use NMITEs IT systems, you must read this policy and follow these rules.

1.5 This document will use clear and concise language, using .gov.uk guidelines. Any technical information will be explained in as simple a format as possible.

1.6 This policy may be amended when deemed appropriate.

2. Scope

2.1 For the purposes of this policy the term 'BYOD' includes, but is not limited to, smart phones, tablets, laptops, PCs, portable storage and any other fixed or mobile computing device.

2.2 This policy applies to all NMITE employees, students, visitors, contractors, agents and anyone else who using NMITE IT services. These individuals will be referred to as 'users' throughout this document.

3. Definitions

3.1 **Information security**: the preservation of the confidentiality, integrity and availability of information.

3.2 **IT Management** – The internal NMITE IT management team. They can be contacted by using the IT Service Desk.

3.3 **Information**: digital data which has meaning.

3.4 **IT Systems**: all software and associated infrastructure

3.5 **Patched** – to solve a problem that a computer system or program has by downloading or installing the latest 'patch' or 'update' from the software provider.

4. Legislative Context

4.1 NMITE must meet its obligations under the Data Protection Act, and the General Data Protection Regulation (GDPR), which governs the security, processing and retention of personal data.

5. Policy - Principles

5.1 NMITE provides at least one corporate device for any member of staff or student connecting to its digital services. Therefore, the requirement for a user to work on a personal device should be minimal.

5.2 Users are strongly encouraged to utilise existing NMITE IT solutions to support teaching, research, study and other NMITE related work.

5.3 NMITE reserves the right to refuse, prevent or withdraw access to services and data where it considers there to be an unacceptable risk to security, data integrity or NMITE policy.

5.4 Anyone using BYOD must adhere to other relevant IT NMITE policies.

6. Policy - Procedure

6.1 Where a corporate device has malfunctioned and is not available, a user should ask the IT Service Desk for a spare machine before attempting to use personal equipment.

6.2 If using a BYOD is considered necessary, users must ensure that the operating system, any antimalware, and security software on the device is the latest version and is fully patched.

6.3 Staff must report the loss of any personally owned device to IT if it is within the scope of this policy so the risk of a data breach can be assessed.

6.4 Staff owned devices that are also used for personal purposes should not be used to download personal or commercially sensitive NMITE data.

6.5 Personal or commercially sensitive NMITE data should only be transmitted using NMITE provided devices and in an appropriately secure fashion.

6.6 Personal file stores and cloud-based data repositories must not be used to store NMITE data.

6.7 When using BYOD, access to NMITE digital resources will be controlled via NMITE approved applications, e.g., Outlook for IOS or Android (to access email). These applications may store local data on a user's personal device. In the event of a security breach that data will be removed/ wiped remotely. NMITE will not interfere with other data on the device.

6.8 The NMITE IT Service Desk is available if you need any IT help with corporate devices. The Service Desk will only help a user connect a BYOD to the corporate Wi-Fi, normally no other support will be available for personal devices. Only in exceptional circumstances will more help be given. This must be requested using the IT Service Desk, via escalation to IT management, for a decision.

7. Responsibility

7.1 Information security remains the responsibility of all NMITE staff, but the following specific responsibilities are assigned to the following individuals and groups:

7.2 The Head of IT is responsible ensuring that all NMITE IT systems, networks and databases comply with the principles of good information security.

7.3 The IT department is responsible for ensuring that IT systems they manage are configured appropriately and used effectively.

7.4 All users of IT must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects its confidentiality, integrity and availability. This includes the use of personally owned devices to access, store or transmit NMITE owned data.

7.5 All users are responsible for accessing and engaging with all information security training and guidance provided by NMITE.

7.6 NMITE takes no responsibility for maintaining, repairing, insuring or otherwise funding BYODs.

7.7 NMITE will not be responsible for any loss or damage resulting from any support given or advice provided.

8. Implementation / Communication Plan

8.1 This policy will be initially communicated to managers via Executive Board emails. Further dissemination will then take place as part of the broader plan to use all available communication channels to raise information security awareness among all staff.

9. Exceptions to this policy

9.1 As this policy outlines the key principles of good BYOD practice exceptions to its principles and procedures are not expected. Any individual who wishes to use a personally owned device for purposes not allowed by this policy, for example, to access store or transmit sensitive information must seek the prior approval of NMITE IT management.

10. Consequences of breaching this policy

10.1 Refer to the NMITE disciplinary policy